

ICS 351: Today's plan

- Simple Network Management Protocol

system administration

- suppose a system administrator has to manage a large number of machines
- for example, three web servers, a DHCP server, a backup server, a Network Attached Storage (NAS) server, a mail server, and a few printers
- a large KVM might be useful, but also has limitations:
 - all the servers must be in close physical proximity
 - there cannot be multiple, remote consoles
 - there is no way to get alerts from systems that need attention

Simple Network Management Protocol

- SNMP uses the network to report status information and alerts about remote systems
- SNMP messages are carried over UDP
- values can be loaded on demand (pull model), but when needed and configured appropriately, alerts are sent independently by the systems being managed (push)

SNMP

Management Information Base

- SNMP needs a machine-independent way to indicate which item of information is being requested or sent
- logically, the entire universe of information that can be accessed is built into a large tree: the Management Information Base or MIB
- the tree is extensible so individuals and organization can add their own subtrees -- private MIBs
- the tree is universal and known to all

navigating the MIB

- the path through the tree is sufficient to indicate one specific item (corresponding to a variable in a programming language)
- the path through the tree can be indicated by a sequence of numbers, the number of left siblings of the path being taken
- for example, 0.2.7.5.14.1.7.0 is such an Object Identifier (OID)
- OIDs are useful for enumerating arrays of objects, e.g., network interfaces, routing table entries

SNMP programs

- a network management station is used by the system administrator to monitor multiple systems
- a management agent must run on every managed device, get the required information, and provide it on request

SNMP basic operation

- the network management station may send GET requests to get one or more objects from specific agents
- the network management station may also send SET requests to modify one or more objects on specific agents
- agents will send TRAP or INFORM alerts to network management stations that they have been configured to alert
- because it uses UDP, SNMP (like DNS) cannot assume that its operations will be successful.

examples

- sample MIB:
http://uw714doc.sco.com/en/SDK_dmi/DMI_SNMP
- MIB table retrieval example:
<http://etutorials.org/Networking/network+management>